Evaluation Warning: The document was created with Spire.Doc for Python.

**小邮付管理端（ 2.0.58版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 小邮付管理端 |
| 版本 | 2.0.58 |
| 包名 | com.java.eastcom.psbchnxyfplatform.base |
| 域名线索 | 16条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年5月5日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | jrjg\_2.0\_beta.apk |
| 文件大小 | 22.0MB |
| MD5值 | 9691b1f38a832681ceb855c7e25d8a32 |
| SHA1值 | 21d6166e350dcb2788a072e1c3cfb0627a91ca5e |
| SHA256值 | 1da48a64db1daa7be0de90c3bd649f431d78a4aae0efaa7f737210277b96f48a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小邮付管理端 |
| 包名 | com.java.eastcom.psbchnxyfplatform.base |
| 主活动Activity | com.java.eastcom.psbchn.activity.SplashActivity |
| 安卓版本名称 | 2.0.58 |
| 安卓版本 | 2058 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| jrstjg.post183.net | IP: 182.42.252.55 所属国家: China 地区: Shandong 城市: Jinan  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| zhyx.post183.net | IP: 117.160.16.178 所属国家: China 地区: Henan 城市: Zhoukou  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://zhyx.post183.net:10001/api/  | 摸瓜V1引擎  |
| https://jrstjg.post183.net:10001/api/  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| yay@y.u5vcghyy  | lib/armeabi/libAndroidIDCard.so  |
| jrs@cs.berkeley  | lib/armeabi/libtxmapengine.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 16534188784  | 摸瓜V1引擎  |
| 14947651605  | 摸瓜V1引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=pms 签名算法: rsassa\_pkcs1v15 有效期自: 2020-10-14 09:34:51+00:00 有效期至: 2045-10-08 09:34:51+00:00 发行人: CN=pms 序列号: 0x6821b467 哈希算法: sha256 md5值: 0df253a206b71355185764178e0949b2 sha1值: 039bd8f3779dc517fe680be6b44ab7786b2aaa2c sha256值: 39d29b3f4fc39d4583a0c97333ab920f94fff2cf55547984ad2780e21f4f9236 sha512值: f293199f48965392873b4612d65c80525b573ec2d0cd78baccde5c2ec5df37edb43b042558f588fc1e5d21a0caf3b678673747d67cdd4e036ee52b84f981e778 公钥算法: rsa 密钥长度: 2048 指纹: c6901a666f33e719c45cb4560a5284ea119ad6f8f559a9b4cfd3a47bc6b8985b**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Residence\_permitforHMT\_residents\_Authority\_Page" : "Residence permit for HMT residents Authority Page"  |
| "Thailand\_Driving\_License\_private" : "Thailand Private Car Driving License"  |
| "ams\_appKey" : "334187671"  |
| "ams\_appSecret" : "14ac2acc14844a90809e5e5d204b523f"  |
| "ams\_hotfix\_idSecret" : "334187671-1"  |
| "ams\_hotfix\_rsaSecret" : "MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCP/MzTIVBHLky6QZW+tH6izi63PmCtg63ZhSsb/ogNn5a+0YkduDSx9sXdneovXZV2N2FSKtqmOAA3xwIAuiK2uA71t5C0GeK+eFkJ++/ADNvv9oQTJOgfRwJuCEtvnc5uQcEOHWQbwiVMDWVJCgw5b2qGQWGwa5iefCDRCuVLraTB2n9uZONqhGM7Dhav6ZiIJN5DflEpZQWy6JK2fwg9gMkuqhP8xKTlZqOw4T+XZ54ugp1CTdiv/UBrV09IPn4h0p3Qkdk3nNf/dUUOU9u5V33jfiHJ5vySeJKP27/qnqJl+Z7x7JtoDJt38eSW1Weu5WCZ0gvA6rfUs1ZFzXNhAgMBAAECggEATX3poktQkC6L3sYDWHJ9oRNEMxygHWI8A1BXRiazhFl6YNIWcGc9/PVpwf8GFV3RXaEqgHVN3Z1QCLTTEB8dJadjbbzQZQ11absNeIEdpAeHqtrKdB8tyf+GgD94kealPdOnmfgZc5MGTar78tY0hAjBlOXFNJSDu+/kHX02sIZBdn9ZYUFx9+SuLDqZ3ouf71ZEdnJPA0rK32L8m+K1Dq7e7ctU+Ci8/WnREteO7B/vysFZKZLjNrCvuKNhorFZbU64VsH7zrS85/gbvN8zLyXaJ+qPopqcn0Bf67B1euFLOnEN5MuqljRstW+O4MAicXS/5qDBEejmfIpFwtQ9QQKBgQDN7FUgiubvB/zbP/DEG47gGbq7BxznXx+FzhUQZRvx0L3bgDVsP0cLSTbToJCn4hZ4SKd9Mw9l4J2i4BkMfn303fgOjEB3J9Ud+yCyaC8os/1ZlrsC5VR4iqY+/e0BJG1OBY+8c5PvchCrtDxp1wAjECzAVEle0kSKYLPrAJonSQKBgQCzAK+qF7GFjwYnwPx1DeqfgAOVEuM/9Rh5+ip/TKrBHiKV6W7ZuRveammGiNaI+gXnb9/uQU9TN/pPsPotlFUqm4micHO1ry+DSSp8PlEeTrO7wYv/rpAnvNpS2AG1mPZBVy/Albh5x4ZoMRJjU0Q6cJvyX1MKWn9M5FcUfBBzWQKBgCyyPHP40lFVyYOJaGgYlzV7QDWyQIrT8dKoPZg2ag9dwKfxNydMwM3pUVY0BtH51+i51GjveUsiqvSccbNtjUdmGp6FwMRcR/ze8mTnCj1qe/ZDKkphnqkfZyBLG3NhBbympmFAMP8LIiUy1N4gRa5Wp3ADm31SZIAop0S997fJAoGBAKmoqNaqhlN0b/0V6TJ48jwi9UJCGKnyADT8a3Mkk2Ne0KEOE0bBMCzq5wHgiJZjg10MqE4GEM1rbRBDSZwRz3cG3LjdpI47cOkaW+5OkkwLhEcc9zhrl65STQvgOB6K0Dy2Ckian7Ks7jOq7ya9MRnCycw7lVVm2OlkMzTzMhRhAoGAaF7XCE2G17tmSst39GpQo0F0hca97J6SZZAzAihekWRxkAow0xOqxqaR29sWEF6rh6ix4XtPFZxDRE0F86oAKpI8wwY+/ES+Lr7qNLqGEDAyf9QFnM1HeQ+ywZlQzdhgZC5qWjhY8KoBJY3Bl6wGnow4UgRKxLYYexbk6WkzR5E="  |
| "ams\_httpdns\_secretKey" : "43f677dbad8bb99d15965317a1835619"  |
| "choose\_ukey" : "移动U宝到扫描位"  |
| "conficate\_ukey" : "吞盾"  |
| "eject\_ukey" : "出盾"  |
| "forget\_pwd" : "忘记密码"  |
| "forget\_pwd\_tips" : "请找网点管理员重置密码"  |
| "load\_main\_key" : "加载主密钥"  |
| "load\_work\_key" : "加载工作密钥"  |
| "no\_pwd\_tip" : "密码不能为空！"  |
| "password" : "密 码"  |
| "select\_role\_user" : "选择客户经理"  |
| "updataPwdTitle" : "请尽快修改密码"  |
| "Residence\_permitforHMT\_residents\_Authority\_Page" : "港澳台居民居住证-签发机关页"  |
| "Thailand\_Driving\_License\_private" : "泰国驾驶证-私家车"  |
| "Residence\_permitforHMT\_residents\_Authority\_Page" : "港澳台居民居住證-簽發機關頁"  |
| "Thailand\_Driving\_License\_private" : "泰國駕駛證-私家車"  |
| "choose\_ukey" : "choose ukey"  |
| "conficate\_ukey" : "conficate ukey"  |
| "eject\_ukey" : "eject ukey"  |
| "load\_main\_key" : "load main key"  |
| "load\_work\_key" : "load work key"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.PROCESS\_OUTGOING\_CALLS | 危险 | 拦截拨出电话 | 允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE  | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.STATUS\_BAR | 系统需要 | 禁用或修改状态栏 | 允许应用程序禁用状态栏或添加和删除系统图标 |
| android.permission.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| com.java.eastcom.psbchnxyfplatform.base.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| com.java.eastcom.psbchnxyfplatform.base.AGOO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.java.eastcom.psbchnxyfplatform.base.ACCS | 未知 | Unknown permission | Unknown permission from android reference |
| com.java.eastcom.psbchnxyfplatform.base.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.java.eastcom.psbchnxyfplatform.base.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**